C. REMARKS

Status of the Claims

Claims 1, 6-8, 14, and 19-29 are currently present in the Application, and claims 1, 8, and 14 are independent claims. Claims 1, 8, 14, and 19-20 have been amended, no claims have been canceled, and no claims have been added in this response.

Examiner Interview

Applicants note with appreciation the telephonic interview conducted between Applicants' representative and the Examiner on June 11, 2007. During the telephonic interview, the Examiner and Applicants' representative discussed one of the 103 references (Al-Salqan, U.S. Patent No. 6,549,626). In particular, Applicants' representative discussed that Applicants' "determining" limitation is not taught or suggested by Al-Salqan. No agreement was reached regarding the claims.

Claim Rejections - 35 U.S.C. § 101

Claims 14, 19, 20, and 27-29 stand rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Applicants have amended the claims to direct the claims to statutory subject matter. Support for such amendment may be found in Applicants' specification on page 26, lines 19-25 and, therefore, no new matter is added with such amendment. As such, Applicants request removal of the 101 rejection to claims 14, 19, 20, and 27-29.

Claim Rejections – Alleged Obviousness Under 35 U.S.C. § 103

Claims 1, 6-8, 14, and 19-29 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Al-Salqan (U.S. Patent No. 6,549,626, hereinafter "Al-Salqan") in view of U.S. Department of Commerce (DOC), "Security Requirements for Cryptographic

Modules" (hereinafter "DOC") in view of Hosokawa (U.S. Patent Pub. 2001/0023416, hereinafter "Hosokawa"). Applicants respectfully traverse these rejections.

Per MPEP 2141, patent examiners carry the responsibility of making sure that the standard of patentability enunciated by the Supreme Court and by the Congress is applied in each and every case. The Supreme Court in Graham v. John Deere, 383 U.S. 1, 148 USPQ 459 (1966), stated:

> Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquires may have relevancy. . .

Therefore, per MPEP 2141, the Examiner should follow USPTO Office policy to follow Graham v. John Deere Co. in the consideration and determination of obviousness under 35 U.S.C. 103. As quoted above, the four factual inquires enunciated therein as a background for determining obviousness are as follows:

(A) Determining the scope and contents of the prior art;
(B) Ascertaining the differences between the prior art and the claims in issue;
(C) Resolving the level of ordinary skill in the pertinent art; and
(D) Evaluating evidence of secondary considerations.

Applicants have amended independent claim 1 to further describe Applicants' determination limitation. Support for such amendment may be found in Applicants' specification on page 14, line 29 through page 15, line 4, and on page 18, line 29 through

page 19, line 2 and, therefore, no new matter is added with such amendment. As amended, Applicants' independent claim 1 includes the limitations of:

- receiving, at a security module, a first password corresponding to a software application;
- generating, at the security module, a first mask value based on the first password;
- combining, at the security module, the first mask value with a first encryption key, wherein the first encryption key is derived from a generated key and a known value, the combining resulting in a tied key;
- encrypting, at the security module, the tied key using a second encryption key that is associated with the security module, the encrypting resulting in an encrypted tied key;
- returning the encrypted tied key to the software application;
- storing, by the software application, the encrypted tied key and a hardware security module identifier that identifies the security module;
- determining, by the software application, that the encrypted tied key corresponds to the security module based upon the hardware security module identifier that is stored with the encrypted tied key;
- in response to the determining, sending the encrypted tied key and a second password from the software application to the security module over a computer network, the second password being the same as the first password;
- receiving, at the security module, the encrypted tied key and the second password from the software application;
- in response to receiving the encrypted tied key and the second password, combining, at the security module, the encrypted tied key and the second password, the combining resulting in a recovered tied key;

- generating a second mask value based on the second password;
- separating a recovered encryption key from the recovered tied key using the second mask value, the recovered encryption key including a recovered generated key and a recovered known value; and
- encrypting data provided by the software application using the recovered generated key.

Applicants' software application receives the encrypted tied key and stores the encrypted tied key with a hardware security module identifier that identifies the particular security module (e.g., a serial number), which is useful in a multi-security module environment. In turn, Applicants' invention uses the hardware security module identifier to determine that the encrypted tied key corresponds to the particular security module in order to send the correct encrypted tied key over to the security module.

Al-Salqan stores the encrypted tied key (without a hardware security module identifier), retrieves the encrypted tied key, and decrypts the encrypted tied key using a supplied password. Al-Salqan states:

> "Asymmetric encryptor 242 passes the resulting encrypted key, referred to as a key recovery file, to key recovery file storage 244. Key recovery file storage 244 provides at output 246 the key recovery file, which may be stored by the principal or others to retrieve the key encrypted therein… Referring now to FIG 3, a system for decrypting a key recovery file to produce a key is shown according to one embodiment of the present invention. The key recovery file is received at input 306 and stored in key recovery file storage 310. A key that will decrypt the encryption performed by the asymmetric encryptor 242 of FIG. 2 is supplied at input 304 and stored in key storage 312… Asymmetric decryptor 314

> receives the key recovery file from key recovery file storage 310 and receives the certificate authority's private key from key storage 312. Asymmetric decryptor 314 decrypts the key recovery file using the certificate authority's private key stored in key storage 312 as the key." (col. 4, ln. 67 - col. 5, ln. 31)

As can be seen from the above excerpt, Al-Salqan teaches passing the encrypted key to a storage area or to a user for storage elsewhere. In turn, Al-Salqan receives a key and decrypts the encrypted key, and does not teach or suggest "*storing, by the software application, the encrypted tied key* ***and a hardware security module identifier that identifies the security module***" and "*determining, by the software application, that the encrypted tied key corresponds to the security module* ***based upon the hardware security module identifier that is stored with the encrypted tied key***" as claimed by Applicants. The differences between Applicants' claimed invention and the cited art are non-obvious differences because Al-Salqan does not deal with a system that includes multiple security modules and, therefore, is not concerned with matching a hardware security module identifier with a corresponding security module. The Office Action does not suggest that DOC or Hosokawa teach or suggest such limitations, and indeed DOC or Hosokawa do not teach such limitations.

Therefore, since Al-Salqan, DOC, or Hosokawa do not teach or suggest, either alone or in combination with each other, all the limitations included in Applicants' claim 1 as amended, amended claim 1 is allowable over Al-Salqan in view of DOC in view of Hosokawa.

Claim 8 is an information handling system claim including similar limitations of claim 1 and, therefore, is allowable for

at least the same reasons as claim 1. Claim 14 is a computer program product claim including similar limitations of claim 1 and, therefore, is allowable for at least the same reasons as claim 1.

Each of the remaining claims 6-7 and 19-29 each depend, directly or indirectly, upon one of the allowable independent claims 1, 8, and 14. Therefore, claims 6-7 and 19-29 are each allowable for the same reasons as their respective independent claims.

Conclusion

As a result of the foregoing, it is asserted by Applicants that the remaining claims in the Application are in condition for allowance, and Applicants respectfully request an early allowance of such claims.

Applicants respectfully request that the Examiner contact the Applicants' attorney listed below if the Examiner believes that such a discussion would be helpful in resolving any remaining questions or issues related to this Application.

Respectfully submitted,

By /Leslie A. Van Leeuwen, Reg. No. 42,196/
Leslie A. Van Leeuwen, Reg. No. 42,196
Van Leeuwen & Van Leeuwen
Attorney for Applicants
Telephone: (512) 301-6738
Facsimile: (512) 301-6742